Microsoft DevOps Solutions: Designing and Implementing Logging

IMPLEMENTING LOGGING IN AZURE

John Savill
PRINCIPAL CLOUD SOLUTION ARCHITECT
@NTFAQGuy www.savilltech.com

Learning Objectives

- Assess and configure a log framework
- Design a log aggregation and storage strategy (e.g., Azure Storage)
- Design a log aggregation using Azure Monitor
- Manage access control to logs (workspace-centric/resource-centric)
- Integrate crash analytics (App Center Crashes, Crashlytics)

Module Overview

Types of log in Azure

Log aggregation basics

Resource diagnostic settings

Using Azure Monitor logs

Azure Monitor log RBAC

Logging enables a centralized view and retention of required information.

Organizations may also require granular access to information even when in a central store along with rich analytics.

Log Aggregation

Some components have their own native log store but can be difficult to work with due to various reasons

- Storage locations and format
- Retention
- Permissions
- Integration for analysis, alerting

Ideally logs we care about should be aggregated to a common store

Azure Metrics and Logs

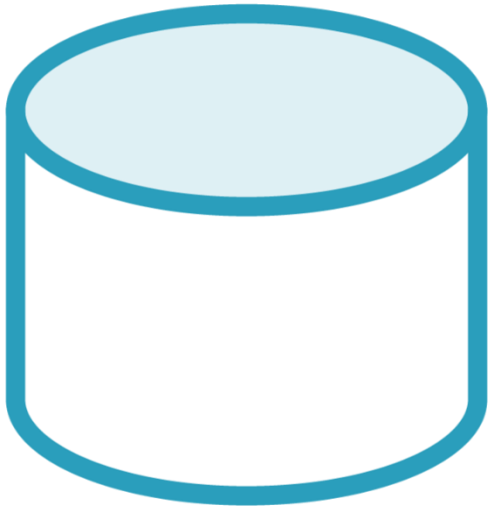
Azure has a large number of metrics and logs

These vary by resource type

Azure resource metrics are stored in the native metrics store for 90 days and can optionally be sent to a target

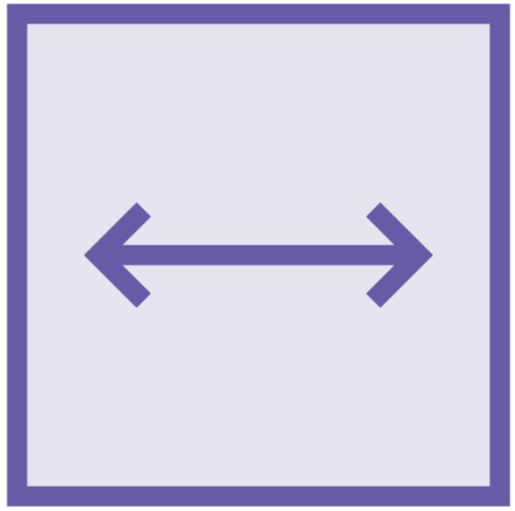
Azure resource logs must be sent to a target

Azure Diagnostic Targets



Azure Storage

Good for long term, cheap retention



Event Hub

Good to send to external solutions

Log Analytics

Good for storage and analytical analysis

Diagnostic Settings

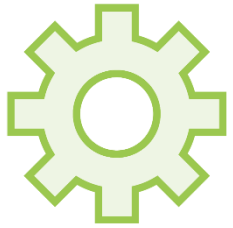
Most resources have a common diagnostic setting option

This enables combinations of targets to be configured for available logs and/or metrics

Multiple sets can be defined to target different instances of a target type

Can be configured through many means including Azure Policy

Sources of Diagnostics

Microsoft Azure Active Directory		Audit Sign-in ...
Subscription		Activity Log (incl Service Health)
Resources		Metrics Logs
Guest/Extension/ Agent		Metrics Logs

Log Analytics Workspace

A subscription can have multiple workspace instances

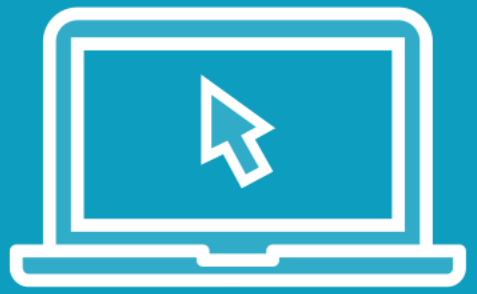
An instance lives within a specific region

You pay based on ingestion, retention and actions performed

Data is stored as tables based on the incoming data

KQL used to query and then visualize

Demo



Interacting with Azure Monitor Logs

Access Control to Logs

Companies may opt for a centralized log strategy or decentralized

Two permissions required to send to a workspace instance from resource

- Microsoft.OperationalInsights/workspaces/read
- Microsoft.OperationalInsights/workspaces/sharedKeys/action

Two access modes area available; workspace-context and resource-context

Access Control Mode

Require workspace permissions

No granular RBAC

Must be granted permission to workspace or tables

Use resource or workspace permissions

Granular RBAC

Default

Summary

- Types of log in Azure
- Log aggregation basics
- Resource diagnostic settings
- Using Azure Monitor logs
- Azure Monitor log RBAC

Next Up: Implementing Crash Analytics